Patch Release Note

Patch 86222-25 For Rapier Switches and AR800 Series Modular Switching Routers

Introduction

This patch release note lists the issues addressed and enhancements made in patch 86222-25 for Software Release 2.2.2 on existing models of Rapier L3 managed switches and AR800 Series L3 modular switching routers. Patch file details are listed in Table 1.

Table 1: Patch file details for Patch 86222-25.

Base Software Release File	86s-222.rez
Patch Release Date	15-April-2003
Compressed Patch File Name	86222-25.paz
Compressed Patch File Size	443760 bytes

This release note should be read in conjunction with the following documents:

- Release Note: Software Release 2.2.2 for Rapier Switches, AR300 and AR700 Series Routers, and AR800 Series Modular Switching Routers (Document Number C613-10313-00 Rev A) available from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- Rapier Switch Documentation Set for Software Release 2.2.1 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- AR800 Series Modular Switching Router Documentation Set for Software Release 2.2.1 available on the Documentation and Tools CD-ROM packaged with your switching router, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.

WARNING: Using a patch for a different model or software release may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.

Some of the issues addressed in this patch include a Level number. This number reflects the importance of the issue that has been resolved. For details on level numbers, please contact your authorised distributor or reseller.

Features in 86222-25

Patch 86222-25 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 02300 Module: Firewall Network affecting: No

If the command ADD FIREWALL POLICY RULE SOURCEPORT=ALL was executed, a value of "65535" was incorrectly displayed for the SOURCEPORT parameter for that rule in the SHOW FIREWALL POLICY command. This issue has been resolved.

PCR: 02400 Module: CORE,FFS,FILE,INSTALL,SCR Network affecting: No

If a problem occurred with NVS, some critical files were lost. As a result, the equipment was forced to load only boot ROM software at boot time. This patch combined with the new version of the boot ROM software (pr1-1.2.0 for the AR700 series) resolves this issue.

PCR: 02530 Module: FIREWALL Network affecting: No

The GBLIP parameter in the ADD FIREWALL POLICY RULE ACTION=NONAT command is optional. However, if the command was executed without the GBLIP parameter set, the command erroneously failed after a CREATE CONFIGURATION command was executed. This issue has been resolved.

PCR: 03111 Module: FIREWALL Level: 1

TCP sessions could fail if the public side of the firewall was using Kerberos and the private side had a very slow connection to the firewall. This issue has been resolved.

PCR: 03134 Module: TCP Level: 2

When using the SET TELNET LISTENPORT command, a fatal error sometimes occurred. This issue has been resolved.

PCR: 03135 Module: SWI Level: 2

The TYPE parameter in the SET SWITCH L3FILTER command was not written to the script file correctly if MATCH was set to NONE. This issue has been resolved.

PCR: 03143 Module: VRRP Level:

When the PRIORITY parameter in the SET VRRP command was changed, it was not set correctly when a link was reset. This issue has been resolved.

PCR: 03145 Module: IPG Level: 4

The SET IP ROUTE FILTER command was not processing some parameters. This issue has been resolved.

PCR: 03148 Module: IPG Level: 3

If the Gratuitous ARP feature was enabled on an IP interface, and an ARP packet arrived, (either ARP request, or reply) that had a Target IP address that was equal to the SenderIP address, then the ARP cache was not updated with the ARP packet's source data. This issue has been resolved.

PCR: 03160 Module: STP Level: 2

Executing the PURGE STP command caused fatal error. This issue has been resolved.

PCR: 03171 Module: DVMRP, IPG Level: 3

DVMRP was erroneously forwarding packets to a VLAN with a downstream neighbour. This issue has been resolved.

PCR: 03173 Module: CORE, NTP Level: 3

The default NTP polling interval was set to 64 seconds, not the correct interval of 128 seconds. This issue has been resolved.

PCR: 03174 Module: IPG Level: 2

This PCR corrects issues that arose with PCR 02203. When the DNS request forwarding queue failed to accept a new DNS request message (possibly due to overloading), an attempt was made to close the UDP sessions for both the primary and secondary name servers. This caused a restart if either one of these servers did not exist, or the UDP session had failed to open. This issue has been resolved.

PCR: 03180 Module: IPG Level: 3

If all 32 VLAN interfaces had IP addresses attached, only 31 VLANs could be multihomed. Now all 32 VLAN interfaces with IP addresses can be multihomed.

PCR: 03202 Module: CORE Level: 3

There are two sources of time kept in the device. The real time clock, and the milliseconds since midnight (msSinceMidnight). The msSinceMidnight can reach midnight slightly before the real time clock which means that the value of the msSince Midnight is larger than the number of milliseconds in a day. This meant that at midnight, the elapsed time since the time-to-live value for the Firewall and IP-NAT TCP sessions appeared very large and Firewall and IP-NAT sessions were prematurely aged out. This issue has been resolved by pausing the msSince Midnight variable at midnight to wait for the real time clock to catch up.

PCR: 03217 Module: DVMRP Level: 2

If a DVMRP interface was deleted and then added again, DVMRP routes associated with this interface were not reactivated. This issue has been resolved.

PCR: 03218 Module: DVMRP Level: 2

Some issues with DVMRP forwarding have been resolved.

PCR: 03236 Module: IPG Level: 3

IGMP queries were being sent after IGMP was disabled. This issue has been resolved.

PCR: 03240 Module: OSPF Level: 2

A fatal error occurred when OSPF was under high load. This issue has been resolved.

PCR: 03253 Module: FIREWALL Level: 2

Inbound TCP sessions through the firewall (e.g. Telnet and FTP) failed when the PORT parameter was set to ALL in the SET FIREWALL POLICY RULE command. This issue has been resolved.

PCR: 03255 Module: FIREWALL Level: 3

The firewall doubled the IPSPOOF event timeout from 2 minutes to 4 minutes. This issue has been resolved.

PCR: 03302 Module: SWI Level: 3

Following a period of high traffic load, the CPU utilisation would occasionally fail to drop below 40%. This issue has been resolved.

PCR: 03314 Module: SWI Level: 2

Layer 3 filters that matched TCP or UDP port numbers were being applied to the second and subsequent fragments of large fragmented packets. This issue has been resolved.

PCR: 03332 Module: TTY Level: 2

A log message is now created when a user is forced to logout from an asynchronous port when another user (i.e. someone connected via Telnet) resets the asynchronous connection with the RESET ASYN command.

PCR: 03346 Module: SNMP Level: 4

Sometimes the *Agent Address* field in SNMP traps was not the same as the IP source address. This meant that sometimes the NMS did not send an alarm to the network manager when traps were received from switches. This issue has been resolved.

PCR: 03368 Module: SWI Level: 2

Layer 2 packets transmitted out of the mirror port were being tagged erroneously. This issue has been resolved.

PCR: 03378 Module: DHCP Level: 2

DHCP sometimes suffered a fatal error when a range of IP addresses was destroyed. This issue has been resolved.

PCR: 03385 Module: FILE, INSTALL, SCR Level:

Critical files (*prefer.ins*, *config.ins* and *enabled.sec*) are now copied from NVS to FLASH at boot time if they do not exist in FLASH, or if the NVS version of the file is different from the FLASH version.

PCR: 03386 Module: SWI Level: 2

If the SET SWITCH L3FILTER MATCH command had nothing specified for the IMPORT and EMPORT parameters, and there was an existing match entry in the filter table, the new filter was not added correctly. Filter match entries are now accepted regardless of the order in which they are entered into the table.

PCR: 03388 Module: DHCP Level: 3

The DHCP lease *Expiry* time showed incorrectly in the SHOW DHCP CLIENT command when the lease straddled across multiple months and years. This issue has been resolved.

PCR: 03402 Module: IPG Level:

IP routes deleted from the route cache occasionally caused a fatal error. This issue has been resolved.

Features in 86222-24

Patch file details are listed in Table 2:

Table 2: Patch file details for Patch 86222-24.

Base Software Release File	86s-222.rez
Patch Release Date	6-Mar-2003
Compressed Patch File Name	86222-24.paz
Compressed Patch File Size	433360 bytes

Patch 86222-23 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 02071 Module: NTP Network affecting: No

When a NTP packet was received from an NTP server (mode 4) the router acted as a client, and sent a reply back to the server, but did not remove the peer association. This meant that the Dynamic Peers list, viewed using the SHOW NTP command, displayed incorrect dynamic peer associations. This issue has been resolved.

PCR: 02202 Module: FIREWALL/IP NAT Network affecting: No

Previously, when Firewall or IP NAT was enabled, any fragmented IP packets had to be reassembled so they could be processed. If the fragments could not be reassembled, the packet was dropped. Reassembly could only occur if the combined packet (IP header, and protocol header, and data) was no more than 1800 bytes. An additional limit of no more than eight fragments was also imposed. This PCR implements enhanced fragment handling for Firewall and IP NAT. Each module can now be configured to process fragmented packets of specified protocol types without needing to reassemble the packet. The number of fragments a packet may consist of is also configurable. This enhanced fragment handling is disabled by default.

To enable enhanced fragmentation for Firewall, use the command:

```
ENABLE FIREWALL POLICY=policy_name
   FRAGMENT={ICMP|UDP|OTHER}
```

To enable enhanced fragmentation for IP NAT, use the command:

```
ENABLE IP NAT FRAGMENT={ICMP|UDP|OTHER}
```

To disable enhanced fragmentation for Firewall, use the command:

```
DISABLE FIREWALL POLICY=policy_name
   FRAGMENT={ICMP|UDP|OTHER}
```

To disable enhanced fragmentation for IP NAT, use the command

```
DISABLE IP NAT FRAGMENT={ICMP|UDP|OTHER}
```

To configure the number of fragments permitted per packet for Firewall, use the command:

```
SET FIREWALL FRAGMENT=8...50
```

To configure the number of fragments permitted per packet for IP NAT, use the command:

```
SET IP NAT FRAGMENT=8...50
```

TCP has been excluded from this enhancement because TCP has the MSS (Maximum Segment Size) parameter for segment size control. Also, for PPPoE interfaces with a reduced MTU of 1492, a previous enhancement in PCR 02097 ensures that TCP MSS values in sessions carried by a PPPoE interface are clamped to a value that prevents fragmentation.

PCR 02116 Module: IPG PING Network affecting: No

When pinging to a remote IP address with two or more different cost routes, if the preferred route became unavailable, the ping failed to switch to the less preferred route until the ping was stopped and restarted. This issue has been resolved.

PCR: 02371 Module: FIREWALL Network affecting: No

When the system time was set to a time that was before or significantly after the current time, Firewall sessions were prematurely deleted. This issue has been resolved.

PCR: 03011 Module: OSPF Network affecting: No

When the router priority was changed on a dynamic OSPF interface, the new priority did not appear in the output of the SHOW OSPF NEIGHBOUR command on neighbouring routers. The new priority only showed after the RESET OSPF command was executed on the neighbouring routers. This issue has been resolved.

PCR: 03026 Module: IPG Network affecting: No

After setting the IGMP query timer with the SET IP IGMP command, and saving the configuration, the IGMP Other Querier timeout was not set to the correct value after a restart. This issue has been resolved.

PCR: 03027 Module: DHCP Network affecting: No

Entries in the process of being reclaimed as static entries (and waiting for the remote IP to become routable), were disrupting the reclaim process. This prevented further entries from being reclaimed. DHCP static entries are now fully subject to normal reclaim processing.

PCR: 03032 Module: SWI Network affecting: No

If the ENABLE IP IGMP command was executed before the ENABLE SWITCH L3FILTER command, Layer 3 filtering did not discard packets destined for the CPU. This issue has been resolved.

PCR: 03035 Module: OSPF Network affecting: No

Link state advertisements could incorrectly show an area as a stub area. This happened during the time when a Direct Route (DR) was removed from a configuration and before a Direct Backup Route (BDR), or an Other Direct Route (Other DR) was elected. This issue has been resolved.

PCR: 03040 Module: IPG Network affecting: No

Sometimes IP flows were not deleted correctly when both directions of the flow were in use. This issue has been resolved.

PCR: 03065 Module: SWI Level: 2

When the TX cable was unplugged from a fibre port the operating status was incorrectly reported as *UP*. This issue has been resolved.

PCR: 03067 Module: DHCP Level: 1

When replying to a DHCP REQUEST that had passed through a DHCP relay, the broadcast bit of DHCP NAK messages was not being set. This issue has been resolved in accordance with RFC2131.

PCR: 03080 Module: DVMRP

DVMRP was not updating the downstream forwarding state correctly. This issue has been resolved.

PCR: 03095 Module: DHCP Level: 2

DHCP policies are no longer stored in alphabetical order in the DYNAMIC CONFIGURATION script because this did not work when the DHCP INHERIT parameter was used.

PCR: 03122 Module: SWI Level: 2

When a static ARP was added to a trunk group, a software restart could occur. This issue has been resolved.

Features in 86222-23

Patch file details are listed in Table 3.

Table 3: Patch file details for Patch 86222-23.

Base Software Release File	86s-222.rez
Patch Release Date	16-Jan-2003
Compressed Patch File Name	86222-23.paz
Compressed Patch File Size	947772 bytes

Patch 86222-23 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 02166 Module: FIREWALL Network affecting: No

Locally generated ICMP packets, such as unreachable messages, were not passed out through public interfaces when the packet that caused the message was not recorded by the firewall. This may occur, for example, if the packet passed between two public interfaces. This issue has been resolved.

PCR: 02491 Module: IPG Network affecting: No

The ARP cache is now updated when a gratuitous ARP request or reply packet is received.

PCR: 02574 Module: DVMRP Network affecting: No

Some change actions, and the resending of prune messages were not operating correctly. This issue has been resolved.

PCR: 02586 Module: CORE, FFS, FILE, INSTALL, SCR Network affecting: No

Reverses PCR 02400.

PCR: 02587 Module: OSPF Network affecting: No

When OSPF was enabled on startup, an OSPF interface would sometimes stay in the DOWN state. This issue has been resolved.

PCR: 03012 Module: TTY Network affecting: No

Logging out from a Telnet session caused the switch to restart. This issue has been resolved.

Features in 86222-22

Patch file details are listed in Table 4.

Table 4: Patch file details for Patch 86222-22.

Base Software Release File	86s-222.rez
Patch Release Date	12-Dec-2002
Compressed Patch File Name	86222-22.paz
Compressed Patch File Size	957598 bytes

PCR 02136 Module: FIREWALL Network affecting: No

The firewall was blocking outbound ICMP packets when the associated private interface had a 'deny all' rule. The passing of ICMP packets should be controlled by the ICMP_FORWARDING and PING parameters. This issue has been resolved.

PCR 02184 Module: FFS FILE TTY Network affecting: No

This patch supersedes PCRs 02073, 02081, 02086 and 02105. In addition to enhancements in the preceding PCRs, this PCR now also resolves the following issues:

- If a compaction was started within 60ms of a file write commencing, the file being written was placed in the wrong location in the file system. This led to file corruption during subsequent compactions.
- If a file load occurred during compaction, an incomplete copy of the file was loaded. The load also put the file into the wrong part of the file system once the compaction had moved beyond the part of the file that had been loaded.
- A fatal error occurred during compaction if a file was marked as deleted when it was being transferred.

- Sometimes during compaction when the file system was erasing blocks belonging to deleted files, one of the files was transferred rather than deleted. However, its directory entry was deleted, so the file was not visible with a SHOW FILE command but was visible with a SHOW FFILE command.
- During compaction if the amount of free space was less than two erase blocks (including the "spare" erase block), the file system erroneously reported that a large amount of space was available for a new file due to an underflow problem. When a new file was written it would corrupt existing data.
- If the file system was completely full and the deletion of a single file led to a compaction, the file system reported that it was continually compacting. This was because it was repeatedly searching through a linked list of file headers.
- A byte of data from FLASH was incorrectly returning the value 0xFF.
- When a file was renamed using upper case letters, the renamed file did not appear in the file directory but did appear in FLASH. Also, if a SHOW FFILE CHECK command was executed after renaming the file, the file system would appear to hang. All file names must now be lower case.
- Multiple TTY sessions could edit the same file. This caused unpredictable behaviour when the TTY sessions closed the files.

A new command, SHOW FFILE VERIFY, has been added. This command steps through the file system headers starting with file zero and finishing at the end of the last reachable file. It then verifies that all FLASH locations from the end of the last reachable file to the beginning of file zero are in an erased state. Errors are reported as they are found.

PCR 02192 Module: IP Network affecting: No

The source IP address in DVMRP *prune* and *graft* messages was incorrect. This issue has been resolved.

PCR: 02241 Module: FIREWALL Network affecting: No

Firewall subnet NAT rules were not working correctly from the private to the public side of the firewall. Traffic from the public to private side (destined for subnet NAT) was discarded. These issues have been resolved. ICMP traffic no longer causes a RADIUS lookup for access authentication, but is now checked by ICMP handlers for attacks and eligibility. If the ICMP traffic matches a NAT rule, NAT will occur on inbound and outbound traffic. HTTP 1.0 requests sometimes caused the firewall HTTP proxy to close prematurely. Cached TCP sessions were sometimes not hit correctly. These issues have been resolved.

PCR: 02359 Module: IPG Network affecting: No

When an IP Multihomed interface was used as an OSPF interface, neighbour relationships were only established if the IP interface for OSPF was added first in the configuration. Now, OSPF establishes neighbour relationships regardless of the IP Multihomed interface configuration order.

PCR: 02395 Module: VRRP, TRG Network affecting: No

The SHOW VRRP command now shows the number of trigger activations for the Upmaster and Downmaster triggers.

PCR: 02396 Module: DHCP Network affecting: No

DHCP RENEW request messages are now unicast (as defined in the RFC), not broadcast.

PCR 02400 Module: CORE, FFS, FILE, INSTALL, SCR Network affecting: No

If a problem occurred with NVS, some critical files were lost. As a result, the equipment was forced to load only boot ROM software at boot time. This patch combined with the new version of the boot ROM software (pr1-1.2.0 for the AR700 series) resolves this issue.

PCR 02408 Module: SWI Network affecting: No

The EPORT parameter in the SHOW SWITCH L3FILTER ENTRY command was displaying incorrectly after an issue was resolved in PCR02374. The command now displays correctly.

PCR: 02427 Module: DHCP Network affecting: No

DHCP entry reclaim checks are now delayed by 10 seconds if the entry is unroutable because the interface is not up.

PCR: 02463 Module: DVMRP, IPG Network affecting: No

Support for multi-homed interfaces has been added.

PCR 02465 Module: TTY Network affecting: No

Under some circumstances a fatal error occurred if a large amount of data was pasted onto the command line. This issue has been resolved.

PCR: 02489 Module: SWI Network affecting: No

When the switch was under heavy learning load, some MAC address were lost. This issue has been resolved.

PCR 02506 Module: OSPF, IPG Network affecting: No

In the ADD IP ROUTE FILTER command, when the optional parameter INTERFACE was included, the filter was not applied to the flooding of OSPF external LSAs. Also, in the command SHOW IP ROUTE FILTER, the output of the interface name was truncated when the name was more than six characters long. These issues have been resolved.

PCR: 02509 Module: DVMRP Network affecting: No

The source net mask has been removed from DVMRP *prune*, *graft* and *graft-ack* messages.

PCR 02526 Module: DVMRP Network affecting: No

Under some circumstances, multiple default routes were created for DVMRP. This issue has been resolved.

PCR 02538 Module: DVMRP Network affecting: No

The source mask is now always 0xffffffff in the DVMRP forwarding table.

The temporary route in the DVMRP route table was not displaying correctly. This issue has been resolved.

An IGMP entry was erroneously added for the reserved IP address. This issue has been resolved.

Features in 86222-21

Patch file details are listed in Table 5:

Table 5: Patch file details for Patch 86222-21.

Base Software Release File	86s-222.rez
Patch Release Date	03-Oct-2002
Compressed Patch File Name	86222-21.paz
Compressed Patch File Size	408864 bytes

Patch 86222-21 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 02167 Module: FIREWALL Network affecting: No

Locally generated ICMP messages, that were passed out through a firewall interface because they were associated with another packet flow, had their source address changed to that of the associated packet flow and were also forwarded with incorrect IP checksums. This only occurred when there was no NAT associated with the packet flow. This issue has been resolved.

PCR: 02236 Module: FIREWALL Network affecting: No

Sometimes the retransmission of an FTP packet was not permitted through the Firewall. This issue has been resolved.

PCR: 02245 Module: VRRP Network affecting: No

VRRP returned an incorrect MAC address for an ARP request. This issue has been resolved.

PCR: 02327 Module: IPG/FIREWALL Network affecting: No

In some situations, multihomed interfaces caused the Firewall to apply NAT and rules incorrectly when packets were received from a subnet that was not attached to the receiving interface. This issue has been resolved.

PCR: 02329 Module: DHCP Network affecting: No

An ARP entry for a host has been removed whenever a DHCP DISCOVER or DHCP REQUEST message is received from the host. This allows for clients changing ports on a switch.

PCR: 02332 Module: IPSEC Network affecting: No

The sequence number extracted from the AH and ESP header was in the wrong endian mode, which caused an FTP error with IPSEC anti-replay. This issue has been resolved.

PCR: 02343 Module: PPP Network affecting: No

When acting as a PPPoE Access Concentrator (AC), if a PPPoE client sent discovery packets without the "host-unique" tag, the discovery packets sent by the AC were corrupted. This issue has been resolved.

PCR: 02368 Module: IPG/IGMP Network affecting: No

IGMP failed to create an automatic IGMP membership with no joining port when it received multicast data that no ports were interested in, when IP *TimeToLive* was set to 1 second. Also, IGMP erroneously sent a query on an IGMP enabled IP interface even when IGMP was disabled. These issues have been resolved.

PCR: 02374 Module: SWI Network affecting: No

In the ADD SWITCH L3FILTER command, the EPORT parameter incorrectly accepted the value 62-63 as multicast and broadcast ports 63-64. This issue has been resolved.

PCR: 02397 Module: DVMRP Network affecting: No

After a prune lifetime had expired, the interface was not joined back to the DVMRP multicast delivery tree. This issue has been resolved.

PCR: 02404 Module: IPG Network affecting: No

DVMRP multicast forwarding failed to send tagged packets to a tagged port. Packets were erroneously sent untagged to tagged ports. This issue has been resolved.

Features in 86222-20

Patch file details for Patch 86222-20 are listed in Table 6:

Table 6: Patch file details for Patch 86222-20.

Base Software Release File	86s-222.rez
Patch Release Date	23-Aug-2002
Compressed Patch File Name	86222-20.paz
Compressed Patch File Size	397708 bytes

Patch 86222-20 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01226 Module: IGMP Network affecting: Yes

The IGMP specific query sent by the router/switch now contains the correct default response time of 1 second. Also, *ifOutOctets* in the VLAN interface MIB now increments correctly.

PCR: 01270 Module: APPLE Network affecting: No

If a port did not belong to an ethernet interface, or was not directly connected to the seed port it could not receive advertised router numbers. This issue has been resolved.

PCR: 01285 Module: OSPF Network affecting: No

When an interface went down (or was disabled) on an AS border router, the external routes were not removed from the routing domain. Such routes are now removed by premature aging.

PCR: 02024 Module: IPG Network affecting: No

Proxy Arp can now be used on VLAN interfaces.

PCR: 02122 Module: FIREWALL Network affecting: No

A fatal error sometimes occurred if a TCP session originating on the public side of the firewall sent packets before the session was established with the host on the private side of the firewall. This issue has been resolved.

PCR: 02128 Module: FIREWALL Network affecting: No

Some FTP packets handled by the firewall were forwarded with incorrect sequence numbers, causing FTP sessions to fail. This issue has been resolved.

PCR: 02150 Module: CORE, SNMP Network affecting: No

When passing 64-bit counters in an SNMP packet, only the lower 32 bits were passed. Now the full 64 bits of the counter will be returned if all are required.

PCR: 02158 Module: FIREWALL Network affecting: No

When a TCP RST/ACK was received by a firewall interface, the packet that was passed to the other side of the firewall lost the ACK flag, and had an incorrect ACK number. This issue has been resolved.

PCR 02161 Module: IPG Network affecting: No

The IP Filter SIZE parameter was not being applied correctly. This issue has been resolved.

PCR 02162 Module: IPG Network affecting: No

The SET IP FILTER command would not update the SIZE parameter correctly. This issue has been resolved.

PCR 02172 Module: IPG Network affecting: No

The TOS field in IP packets was not being processed by IP POLICY filters with an identifier greater than 7. This issue has been resolved.

PCR: 02174 Module: FIREWALL Network affecting: No

A feature has been added that makes pings pass from the source IP address of the public interface to the IP address on the private interface in the firewall.

PCR: 02195 Module: SWI Network affecting: No

If a port on a Rapier 48 or Rapier 48 *i* went down, some associated entries were not promptly removed from the forwarding, Layer 3 and default IP tables. This issue has been resolved.

PCR: 02198 Module: DHCP Network affecting: Yes

This PCR includes the following enhancements:

- A new command, SET DHCP EXTENDID allows for multiple DHCP clients, and handling of arbitrary client IDs on the server.
- Static DHCP entries now return to the correct state when timing out.

- DHCP entry hashes now have memory protection to prevent fatal errors.
- DHCP client now retransmits XID correctly.
- Lost OFFER messages on the server are now handled correctly.
- The DHCP server now correctly handles DHCP clients being moved to a different interface on the DHCP server after they've been allocated an IP address.

PCR: 02203 Module: IPG Network affecting: No

Responses to DNS requests received by a DNS relay agent, and forwarded to the DNS server, were returned to the requester with a source IP address of the DNS server rather than the DNS relay agent. This issue has been resolved.

PCR: 02208 Module: LOG Network affecting: No

Log messages are no longer stored in NVS.

PCR: 02214 Module: IPG Network affecting: No

A buffer leak occurred when a large number of flows (over 4000) were in use and needed to be recycled. This issue has been resolved.

PCR: 02215 Module: FILE Network affecting: No

When the only feature licence in the feature licence file was disabled, the licence file stored on FLASH memory did not change. This was due to a previous enhancement in PCR 02184 which prevented existing files being deleted before a new version was stored. This issue has been resolved.

PCR: 02220 Module: SWI Network affecting: No

The EPORT parameter in the ADD SWITCH L3FILTER ENTRY and SET SWITCH L3FILTER ENTRY commands was matching multicast and broadcast packets with software filtering. This issue has been resolved.

PCR: 02224 Module: SWI Network affecting: No

Some switch chip register values have been changed to improve QoS support on Rapier G6 and Rapier G6f switches.

PCR: 02229 Module: IPG Network affecting: No

The PURGE IP command now resets the IP route cache counters to zero.

PCR: 02242 Module: IPG Network affecting: No

On a Rapier 24, adding an IP interface over a FR interface caused an ASSERT debug fatal error. This issue has been resolved.

PCR: 02246 Module: VRRP Network affecting: No

The ARL entry for the virtual router MAC was incorrectly showing a numerical value. The entry now shows the CPU's port value.

PCR: 02250 Module: FIREWALL Network affecting: No

Sometimes the Firewall erroneously used NAT. This issue has been resolved.

PCR: 02259 Module: DHCP, IPG Network affecting: No

A dual Ethernet router was incorrectly accepting an IP address from a DHCP server when the offered address was on the same network as the other Ethernet interface. An error is now recorded when DHCP offers an address that is in the same subnet as another interface.

PCR: 02260 Module: TTY Network affecting: No

When a '\n'(LF) character was received, the router/switch did not recognise this as the termination of a command over Telnet. This issue has been resolved.

PCR: 02262 Module: DNS Network affecting: No

Responses to MX record requests were not handled correctly if the preferred name in the MX record differed from the one that was requested. This issue has been resolved.

PCR: 02263 Module: VRRP Network affecting: No

The virtual MAC address was used as the source MAC for all packets forwarded on an interface associated with a Virtual Router (VR). This was confusing when multiple VRs were defined over the same interface because only one virtual MAC address was ever used. The other virtual MAC addresses (for the other VR's) were only used if the source IP address matched the VR's IP address. To avoid this confusion, the system MAC address is now always used unless the source IP address of the packet is the same as the VR's IP address.

PCR: 02264 Module: PIM, DVMRP, SWI Network affecting: No

PIM or DVMRP failed to see any data if IGMP snooping was on and DVMRP or PIM was enabled after the data stream had reached the router/switch. This issue has been resolved.

PCR: 02265 Module: FIREWALL Network affecting: No

MAC address lists were not working with Firewall rules. This issue has been resolved.

PCR: 02268 Module: FIREWALL Network affecting: No

HTTP requests from a fixed IP address were erroneously reported as a host scan attack in the Firewall deny queue. This issue has been resolved.

PCR: 02269 Module: DUART, TM Network affecting: No

Under certain circumstances, the Asyn Loopback Test failed. This issue has been resolved.

PCR: 02274 Module: TPAD Network affecting: No

ARL message interrupts have been re-enabled after a software table rebuild to fix synchronisation of the software forwarding database with the hardware table.

PCR: 02275 Module: OSPF Network affecting: No

Some routes were not added into the OSPF route list, and therefore were not added into the IP route table. This issue has been resolved.

PCR: 02276 Module: FIREWALL Network affecting: No

The CREATE CONFIG command did not save the SOURCEPORT parameter to the configuration file when the low value of the source port range was set to zero. This issue has been resolved.

PCR: 02287 Module: IPG Network affecting: No

Existing IGMP groups were not deleted when IGMP was disabled globally or on the associated interface. This gave the groups very high timeout values. This issue has been resolved.

PCR: 02299 Module: VRRP Network affecting: No

If a packet with a destination IP address equal to a VRRP IP address was received when the router didn't own the IP address, (because it didn't have an interface with that IP address) the router incorrectly tried to forward the packet and send an ICMP "redirect" message to the source. Now, if such a packet is received, it will be discarded and an ICMP "host unreachable" message will be sent to the source.

PCR: 02304 Module: VRRP Network affecting: No

VRRP used the wrong source IP address in ICMP redirects. RFC 2338 states that the source IP address of ICMP redirects should be the IP address that the end host used when making its next hop routing decision. In the case of a packet sent to a VRRP virtual MAC address, this is the primary VRRP IP address associated with the MAC address, provided such a VR exists and is in the master state. This issue has been resolved.

PCR: 02317 Module: IPG Network affecting: No

The SIZE functionality on the IP filter was not working for IP fragmented packets. This issue has been resolved.

Features in 86222-19

Patch file details for Patch 86222-19 are listed in Table 7:

Table 7: Patch file details for Patch 86222-19.

Base Software Release File	86s-222.rez
Patch Release Date	11-Jun-2002
Compressed Patch File Name	86222-19.paz
Compressed Patch File Size	364584 bytes

Patch 86222-19 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 02018 Module: OSPF Network affecting: No

When OSPF was calculating routes from an AS external LSA and the AS external router had two next hops with different metrics, the router erroneously added two routes instead of one route with the best metric. This issue has been resolved. Also, when the two equal cost routes were on the same IP interface, but to different next hops, the router sent the packets to the wrong MAC address. This issue has been resolved.

PCR: 02098 Module: STP Network affecting: No

STP always transmits untagged packets. If a port does not belong to a VLAN as an untagged port, then the port must belong to one VLAN as a tagged port. In this case, STP should transmit VLAN tagged packets out of the port.

PCR: 02123 Module: IPG Network affecting: No

The IP, MASK, and ACTION parameters could not be set with the SET IP ROUTE FILTER command. This issue is resolved when the filter number is specified at the start of the command, for example:

```
SET IP ROUTE FILTER=filter-id IP=ipadd MASK=ipadd
ACTION={INCLUDE|EXCLUDE}
```

where: *filter-id* is the filter number. Filter numbers are displayed in the output of the SHOW IP ROUTE FILTER command.

PCR 02138 Module: SWI Network affecting: No

The built in Self Test Code for all Rapiers, except G6, has been improved to enhance the detection of faults in switch chip external packet memory.

PCR 02140 Module: OSPF Network affecting: No

An AS boundary router advertises AS external LSAs to other routers. However, when the router's configuration changed, either by adding an IP route filter, or by setting its ASEXTERNAL parameter to OFF using the SET OSPF ASEXTERNAL command followed by a restart, its neighbour state could not reach full state. Also, when the router had IP route filters configured, matched routes were not being flooded into other routers. However, these routes should still have been imported into the router's own LSA database, but were not. These issues have been resolved.

PCR 02144 Module: IPG Network affecting:No

The IPG module has been enhanced to support gratiutous ARP request and ARP reply packets.

PCR 02151 Module: IPG Network affecting: No

The Rapier was not detecting invalid checksums in ICMP echo request packets. This issue has been resolved. ICMP echo request packets with invalid checksums are now dropped and the ICMP *inErrors* and *inDiscards* counters are incremented.

PCR 02164 Module: DHCP Network affecting: No

A simple DHCP range MIB and a trap have been added. The trap is triggered when a DHCP request cannot be satisfied. The gateway address and the interface address are sent as trap variables. The range table shows which range was exhausted. A debug variable, *swiDebugBroadcomParityErrors* has been added to the SWI module MIB to count the SDRAM parity errors in the packet memory of the Broadcom switch chip.

PCR 02176 Module: FIREWALL Network affecting: No

Packets traversing in and out of the same public firewall interface were sometimes blocked. The firewall should only control packets passing between a public and a private interface. This issue has been resolved.

PCR 02181 Module: LOAD Network affecting: No

When a file upload was interrupted, the file being uploaded was not unlocked. The file could not be deleted without restarting the router. This issue has been resolved.

PCR 02186 Module: IPG Network affecting: No

RIP was incorrectly sending triggered request packets over VLANs, even on non-demand links. This issue has been resolved.

PCR 02188 Module: VRRP Network affecting: No

When VRRP responded to an ARP request for the VR IP address it was not making an entry in the ARP table and the switch L3 table. This issue has been resolved.

Features in 86222-18

Patch file details for Patch 86222-18 are listed in Table 8:

Table 8: Patch file details for Patch 86222-18.

Base Software Release File	86s-222.rez
Patch Release Date	6-May-2002
Compressed Patch File Name	86222-18.paz
Compressed Patch File Size	342720 bytes

There is no patch release 86222-17 because this patch was withdrawn.

Patch 86222-18 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 02041 Module: SWI Network affecting: No

In some situations, the switch would stop forwarding packets via internal and/or external uplink ports. This issue has been resolved.

PCR: 02073 Module: FILE Network affecting: No

If a flash write error occurred when a file was being written, the file's directory entry was deleted leaving a partial file in flash. Subsequent attempts to write the file failed because a file of the same name already existed. This issue has been resolved.

PCR: 02075 Module: OSPF, IPG Network affecting: No

In configurations containing a large number of OSPF routes, the SPF calculation could take a long time. During this calculation, other events would not be processed. This patch reduces the time required for an SPF calculation and allows the switch to respond to other events in the mean time. This patch also improves the performance of flow cache updates.

PCR: 02081 Module: FILE, FFS Network affecting: No

If the FILE module was required to re-write a file, the existing file would be deleted before the size of the new file was known. This issue has been resolved.

PCR: 02082 Module: OSPF Network affecting: Yes

OSPF virtual links running across a single network segment would accept 0.0.0.0 as the next hop address. This was inherited by derivative routes, making them unusable. This issue has been resolved.

PCR: 02086 Module: FFS Network affecting: No

If a file ended short of an erase block boundary and a compaction was started, the block in which the file was stored was not erased, causing errors when new files were written. Also, if the last file in the filing system ended on or short of an erase block boundary, and a compaction was started, then compaction would fail. These issues have been resolved.

PCR: 02088 Module: SWI Network affecting: No

Port mirroring on the Rapier 48 and 48i was not operating correctly because Destination Lookup Failure (DLF) frames were sent from the mirror port. This issue has been resolved.

PCR: 02095 Module: SWI Network affecting: No

The software routing performance of the Rapier 48 and Rapier 48i has been enhanced.

PCR: 02101 Module: SWI Network affecting: No

The layer 3 hardware table was not sorted properly when it contained a very wide range of IP addresses (eg. 10.0.0.1 - 205.33.3.1). This caused a small number of packets to be routed by software rather than hardware. This issue has been resolved.

PCR: 02104 Module: TRG Network affecting: No

The periodic and time trigger counts were incrementing by two instead of one on each update. This issue has been resolved.

PCR: 02105 Module: FFS Network affecting: No

An error occurred when the FLASH write driver was required to write values that were not long-word aligned and were at the driver's page boundary. The driver attempted to write into the next section of memory. It also attempted to read the status of this section of memory, and misinterpreted the result as a low Vpp voltage. Also, errors occurred during FLASH compaction. These issues have been resolved.

Features in 86222-16

Patch file details for Patch 86222-16 are listed in Table 9:

Table 9: Patch file details for Patch 86222-16.

Base Software Release File	86s-222.rez
Patch Release Date	1-Apr-2002
Compressed Patch File Name	86222-16.paz
Compressed Patch File Size	336952 bytes

Patch 86222-16 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 02092 Module: SWI Network affecting: No

The SET SWITCH L3 FILT command overwrote existing Layer 3 filters. If multiple filter entries existed, this command changed the most recent entry, rather than the one specified. These issues have been resolved. Also, the SET SWITCH L3 FILT command now allows for creation of multiple filter entries with the SETPRIORITY and SETTOS parameters. The Layer 3 filter protocol match now has no limit.

PCR: 02099 Module: DHCP Network affecting: No

A switch sometimes restarted if it was configured with static DHCP entries and was handling a large number of DHCP clients. This issue has been resolved.

Features in 86222-15

Patch file details for Patch 86222-15 are listed in Table 10:

Table 10: Patch file details for Patch 86222-15.

Base Software Release File	86s-222.rez
Patch Release Date	26-Mar-2002
Compressed Patch File Name	86222-15.paz
Compressed Patch File Size	336608 bytes

Patch 86222-15 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 02015 Module: SNMP Network affecting: No

A fatal error occurred when an invalid SNMP message was received. This issue has been resolved.

PCR: 02020 Module: SWI Network affecting: No

When disabling port mirroring the VLAN tagging configuration of other ports was corrupted. This issue has been resolved.

PCR: 02070 Module: CORE Network affecting: No

The TickTimer ran one percent slower than it should have. This issue has been resolved.

PCR: 02079 Module: IPG Network affecting: No

Static ARPs can now be added to tagged vlans.

PCR: 02094 Module: IPG Network affecting: No

When an IP flow table contained the IP flow structure for a spoofed packet, the SHOW IP FLOW command would crash when executed. This issue has been resolved.

Features in 86222-14

Patch file details are listed in Table 11.

Table 11: Patch file details for Patch 86222-14.

Base Software Release File	86s-222.rez
Patch Release Date	28-Feb-2002
Compressed Patch File Name	86222-14.paz
Compressed Patch File Size	335336 bytes

Patch 86222-14 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 02005 Module: IPG Network affecting: No

When telnetting to the switch, the TCP connection was reset, and when the packet was passed to IPG_Forward a fatal error occurred. This patch implements a workaround.

PCR: 02035 Module: VLAN Network affecting: No

The CREATE CONFIG command now correctly configures tagged ports belonging to VLANs not in the default STP.

PCR: 02036 Module: SWITCH Network affecting: No

A new command allows the Layer 3 aging timer to be changed:

SET SWITCH L3AGEINGTIMER=<seconds>

where seconds can be 30 - 43200. After each cycle of the ageing timer, all existing Layer 3 entries with the hit bit set will have the hit bit reset to zero, and all existing Layer 3 entries with the hit bit set to zero will be deleted.

The SHOW SWITCH command output now displays the Layer 3 ageing timer value.

PCR: 02038 Module: PING Network affecting: No

Resolution of PCR 02011 in Patch 12 sometimes caused a fatal error. This issue has been resolved.

PCR: 02039 Module: IPG Network affecting: No

The SHOW IP ROUTE FILTER command output displayed counters for 'passes' and 'include' that were the same. This issue has been resolved. Counters now increment only when a filter is active and do not count interface routes.

PCR: 02040 Module: SWI Network affecting: No

PCR 02019 permitted the reception of packets by the CPU that should have been discarded. This issue has been resolved.

PCR: 02057 Module: FIREWALL Network affecting: No

Firewall TCP timeout values have been reduced for sessions placed in the CLOSED state after receiving a TCP/RESET. This applies to the stateful inspection of firewall sessions only, and not to the TCP module. Previously, PCR 01263 reduced the timeout value for sessions placed in the CLOSED state after a TCP/FIN packet was received.

PCR: 02063 Module: FIREWALL Network affecting: No

Firewall IP access lists were not working correctly. If an IP range was specified without spaces between the IP address and the separating '-' the range would be ignored. Spaces are no longer required. Also, matches were made to addresses covered by a range in an access list if the matching range was numerically the lowest in the list. This issue has been resolved.

Features in 86222-13

Patch file details for Patch 86222-13 are listed in Table 12.

Table 12: Patch file details for Patch 86222-13.

Base Software Release File	86s-222.rez
Patch Release Date	1-Feb-2002
Compressed Patch File Name	86222-13.paz
Compressed Patch File Size	328884 bytes

Patch 86222-13 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 02014 Module: TELNET Network affecting: No

When a Telnet session was terminated without a proper logout, counters recording the number of logins were not correctly decremented. This issue has been resolved.

PCR: 02019 Module: SWI Network affecting: No

If a layer 3 hardware filter for a particular packet type (e.g. Netbeui) was configured, all IP packets destined for the CPU were discarded. This issue has been resolved.

Features in 86222-12

Patch file details for Patch 86222-12 are listed in Table 13.

Table 13: Patch file details for Patch 86222-12.

Base Software Release File	86s-222.rez
Patch Release Date	18-Jan-2001
Compressed Patch File Name	86222-12.paz
Compressed Patch File Size	328528 bytes

Patch 86222-12 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01223 Module: IPG Network affecting: No

If route filters existed and a RESET IP command was executed, some static and interface routes were incorrectly removed if the filters matched. This issue has been resolved.

PCR: 01257 Module: DHCP Network affecting: No

DHCP occasionally caused a fatal error. Also, while an address was in the reclaiming list, a DHCPDISCOVERY message requesting the address made the address disappear. These issues have been resolved.

PCR: 01261 Module: IPG/VRRP Network affecting: No

A fatal error occurred when forwarding IP packets with VRRP enabled. This issue has been resolved.

PCR: 01263 Module: FIREWALL Network affecting: No

The firewall TCP timeout values for sessions in the CLOSED and TIMEWAIT states have been reduced. This only applies to the stateful inspection of firewall sessions and not to the TCP module.

PCR: 01268 Module: SWI Network affecting: No

When a Rapier was under heavy load from software routing (e.g. after a reboot and before the routing tables were refreshed), OSPF could take a long time to converge. This patch gives OSPF packets higher priority to expedite OSPF convergence.

PCR: 01269 Module: SWI Network affecting: No

A new feature permits hardware filtering by the Rapier family based on the Ethernet frame type. The TYPE parameter:

```
TYPE={802|ETHII|SNAP}
```

has been added to the following commands:

ADD SWITCH L3FILTER ENTRY

ADD SWITCH L3FILTER MATCH

SET SWITCH L3FILTER ENTRY

SET SWITCH L3FILTER MATCH

SHOW SWITCH L3FILTER

PCR: 01272 Module: SWI Network affecting: No

A physical port could not be re-enabled once disabled when STP was active. This issue has been resolved.

PCR: 01273 Module: SWI Network affecting: No

The CREATE CONFIG command now includes the STPFORWARDING parameter in generated scripts. The SHOW SWITCH command now displays the setting of STPFORWARDING.

PCR: 01274 Module: SWI Network affecting: No

Refinements were made to the switch chip register settings improving CoS provision with the newer revision of switching silicon on the Rapier 16, Rapier 24 and Rapier 48.

PCR: 01275 Module: FIREWALL Network affecting: No

The firewall was incorrectly forwarding multicast packets originating from a private address in cases where a matching route was defined. This issue has been resolved.

PCR: 01276 Module: SWI Network affecting: No

When the speed of one or more switch ports was forced to a half duplex setting and the ports were then added to a trunk group configured for full duplex operation, the port settings were not overridden by the trunk group speed setting. The trunk group speed setting will now take precedence over the port speed setting.

PCR: 01287 Module: OSPF Network affecting: No

Configuring IP route filters did not stop flooding of AS external LSAs to neigbours at startup. The result was that the neigbour received the AS LSAs and added the corresponding routes into its own routing table. However, after some time (e.g. 1 hour), the AS external LSAs in the neigbour's database disappeared, but the corresponding routes were still in its routing table. This issue has been resolved.

PCR: 01289 Module: VRRP Network affecting: No

The checksum in VRRP advertisements was not being calculated correctly. The calculation was not compatible with the RFC. This issue has been resolved.

PCR: 01290 Module: PPP Network affecting: No

When PPP was running over Ethernet to a client from another vendor, the Maximum Transmission Unit value for the link was not adjusted from the PPP default of 1500 to 1492. This issue has been resolved.

PCR: 01291 Module: IPG(IGMP) Network affecting: No

IGMP did not send the Start Up Query, and the Other Querier Present Timer did not change the Time Out value accordingly if Query Interval was changed. IGMP did not notify other registered parties (PIM and DVMRP) when a port was deleted from a membership group. IGMP reported a membership leave to other parties while it was still waiting for a reply to a group specific query from a leaving member. These issues have been resolved.

PCR: 02003 Module: FIREWALL Network affecting: No

The timeout value for ICMP session entries in the firewall can now be adjusted via the OTHERTIMEOUT parameter of the SET FIRE POLICY command. Note: if the value for OTHERTIMEOUT is set to more than 10 minutes the timeout used for ICMP sessions will default to 10 minutes.

PCR: 02007 Module: DHCP Network affecting: No

When a DHCP server received a DHCP DISCOVERY packet passed by a relay agent, requesting an IP address that did not belong to the subnet the client and the relay agent were attached to, it offered the requested address if it was available. The DHCP server will now only offer an IP address from the subnet that connects the client and the relay agent.

PCR: 02008 Module: TRIGGER Network affecting: No

The first periodic after day trigger boundary (i.e. midnight) did not occur. A range check error occurred due to an incorrect comparison. These issues have been resolved.

PCR: 02011 Module: PING Network affecting: No

Stopping a trace route using STOP TRACE occasionally caused a fatal error. This issue has been resolved.

PCR: 02012 Module: IPG, VLAN, SWI Network affecting: No

IGMP reflooded packets with VLAN tagging were not processed correctly. This issue has been resolved.

Features in 86222-11

Patch file details for Patch 86222-11 are listed in Table 14.

Table 14: Patch file details for Patch 86222-11.

Base Software Release File	86s-222.rez
Patch Release Date	19-Dec-2001
Compressed Patch File Name	86222-11.paz
Compressed Patch File Size	296244 bytes

Patch 86222-11 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01243 Module: SWI Network affecting: No

When a Rapier CPU was handling a large amount of traffic and a busy egress port went down, it was possible for the transmission of packets by the CPU to cease. This issue has been resolved.

PCR: 01265 Module: SWI Network affecting: No

When trunking was in operation, in some instances the switch transmitted tagged packets on untagged trunk ports. This issue has been resolved.

PCR: 01288 Module: SWI Network affecting: No

When a switch port was forced to half duplex mode and the link partner was forced to full duplex mode, it was possible for the switch to enter a state where it was unable to transmit packets. This issue has been resolved.

Features in 86222-10

Patch file details for Patch 86222-10 are listed in Table 15.

Table 15: Patch file details for Patch 86222-10.

Base Software Release File	86s-222.rez
Patch Release Date	29-Nov-2001
Compressed Patch File Name	86222-10.paz
Compressed Patch File Size	295536 bytes

Patch 86222-10 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancement:

PCR: 01264 Module: SWI Network affecting: No

Some switch chip register settings have been optimised to improve the provision of CoS with the newer revision of switching silicon.

Features in 86222-09

Patch file details for Patch 86222-09 are listed in Table 16.

Table 16: Patch file details for Patch 86222-09.

Base Software Release File	86s-222.rez
Patch Release Date	27-Nov-2001
Compressed Patch File Name	86222-09.paz
Compressed Patch File Size	295444 bytes

Patch 86222-09 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01189 Module: STP, SWI Network affecting: Yes

A new feature, STP forwarding, has been added. STP forwarding can be enabled and disabled using the commands:

```
ENABLE SWI STPFORWARD
DISABLE SWI STPFORWARD
```

When STP forwarding is enabled, all STP forwarding is ignored and all BDPUs received on a port are forwarded on all other ports.

PCR: 01242 Module: CORE, SNMP Network affecting: No

The switch now delays sending link traps immediately after a restart to give the link to the trap host time to come up. A similar change has been made for the cold start trap. After a 10s delay, all interfaces which are UP have a link trap generated for them. After that, link traps are sent as normal.

PCR: 01244 Module: SWI, CORE, IPG Network affecting: No

Processing invalid UDP packets caused a memory leak. This issue has been resolved. Additional debugging facilities were added.

PCR: 01246 Module: SWI Network affecting: No

The default setting for the switch port parameter INFILTERING is now OFF, as specified in IEEE802.1Q. A VLAN will still reject these packets if they are not from valid VLAN member ports.

PCR: 01247 Module: IPG Network affecting: No

The IGMP snooping forwarding process now correctly selects outgoing ports when DVMRP is managing the multicast routing information.

PCR: 01248 Module: SWI Network affecting: No

A configuration problem prevented trunking of gigabit ports at 100Mbit speeds. This issue has been resolved. The A39 gigabit copper uplink reverted to autonegotiation after a restart, even if it was configured to a fixed speed. This issue has been resolved. When the port has been configured for a fixed speed, the mode is now set to MDIX, not MDI.

PCR: 01254 Module: PRI Network affecting: No

When an M2 version of the AR020 PRI E1/T1 PIC was installed in a AR040 NSM it was not possible to select the T1 mode of operation regardless of the jumper setting. This issue has been resolved.

PCR: 01256 Module: Firewall Network affecting: No

A fatal error occurred when the firewall discarded disallowed multicast packets. This issue has been resolved.

Features in 86222-08

Patch file details for Patch 86222-08 are listed in Table 17.

Table 17: Patch file details for Patch 86222-08.

Base Software Release File	86s-222.rez
Patch Release Date	09-Nov-2001
Compressed Patch File Name	86222-08.paz
Compressed Patch File Size	291012 bytes

Patch 86222-08 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01201 Module: L2TP Network affecting: Yes

Tunnel creation failed when attempting to establish a point-to-point tunnel from an ATR router (tunnel originator) to another vendor's router. This issue has been resolved.

PCR: 01233 Module: PIM Network affecting: No

When IGMP snooping was enabled, if a member left a group on a port, it could not re-join the group on that port. This issue has been resolved.

Substantial changes have been made to PIM in more recent code releases. These have been retrofitted to 2-2-2 in the patch. Note: these changes have incorporated PCRs 01159 and 01190.

PCR: 01236 Module: PPP Network affecting: No

The PPPoE access concentrator did not stop RADIUS accounting when a PADT termination was received without receiving a proper PPP termination first. This issue has been resolved.

PCR: 01237 Module: SWI Network affecting: No

The dot1dBridge MIB implementation now complies with RFC1493.

Features in 86222-07

Patch file details for Patch 86222-07 are listed in Table 18:

Table 18: Patch file details for Patch 86222-07

Base Software Release File	86s-222.rez
Patch Release Date	26-Oct-2001
Compressed Patch File Name	86222-07.paz
Compressed Patch File Size	250468 bytes

Patch 86222-07 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01018 Module: DHCP Network affecting: No

DHCP now correctly handles request messages containing request list options not supported by the router.

PCR: 01160 Module: IPG,FIREWALL Network affecting: No

The router would accept TCP sessions with destination address the same as the subnet broadcast address for one of the router's interfaces. Firewall-generated packets destined for a subnet broadcast address on one of the routers interfaces would cause a fatal error. These issues have been resolved.

PCR: 01168 Module: HTTP Network affecting: No

A watchdog timout occurred when the router received an HTTP message with an over-length header. Normal HTTP requests would also occasionally cause watchdog timeouts. These issues have been resolved.

PCR: 01182 Module: OSPF Network affecting: No

The OSPF route filter was not filtering out external routes. This issue has been resolved.

PCR: 01193 Module: IPG Network affecting: No

MD5 Authentication now works correctly with RIP packets.

PCR: 01194 Module: L2TP, IPG Network affecting: No

The SET IP LOCAL command caused a fatal error if the router was configured with a default route over an L2TP tunnel, because there was no valid route to the remote IP address of the tunnel. This issue has been resolved.

PCR: 01197 Module: Q931 Network affecting: No

Debug messages are no longer generated when a Q.931 Advise of Charge Notification message is received.

PCR: 01198 Module: TCP Network affecting: No

TCP sessions would get stuck in the FINWAIT2 state if the remote host did not send a FIN message when required. The router now starts a timer when a TCP session enters the FINWAIT2 state and will automatically close the session if the timer expires.

PCR: 01199 Module: IPG Network affecting: No

The SET IP FILTER command was not correctly handling the ICMPTYPE and ICMPCODE parameters. This issue has been resolved.

PCR: 01202 Module: DHCP Network affecting: No

The router will now accept DHCP messages that are greater than or equal to 576 bytes in size, and reject any message smaller than 576 bytes. This operation conforms to RFC 1541.

PCR: 01203 Module: ISAKMP Network affecting: No

ISAKMP quick mode exchanges are now committed if any traffic is received over the newly generated SA. This improves stability in very lossy networks where the commit message may get lost.

PCR: 01204 Module: ISAKMP Network affecting: No

ISAKMP debugging caused a fatal error when the debugging mode was set to ALL and PFS was enabled. This issue has been resolved.

PCR: 01205 Module: PPP Network affecting: No

PPPoE interfaces with IDLE set to ON would not retry active discovery when more data was received if active discovery had previously failed. This issue has been resolved.

PCR: 01206 Module: ISAKMP Network affecting: No

A memory loss occurred when certificates were used by ISAKMP. This issue has been resolved.

PCR: 01207 Module: ISAKMP Network affecting: No

ISAKMP heartbeats are no longer transmitted if the lower layer interface is down. This stops ISAKMP heartbeats from bringing up links in dial-up environments.

PCR: 01209 Module: ISAKMP Network affecting: No

In some conditions it was possible for ISAKMP packets to be lost and not retransmitted. Incoming ISAKMP messages are now validated before stopping retransmission of the previous message.

PCR: 01211 Module: SWI Network affecting: No

The COS_DST bit on ARL for L3 interface should be 0x4 (higher priority) for CPU ports. This has been corrected.

PCR: 01213 Module: TRG, SNMP Network affecting: No

The Trigger Facility was generating a trap with variable { 0 0 }, and was not documented in the ATI enterprise MIB. This issue has been resolved. The MIB object *triggerLastTriggerActivated* ({ enterprises(1) alliedTelesyn(207) mibObjects(8) brouterMib(4) atrouter(4) modules(4) trigger(53) 1 }) has been defined, to record the trigger number of the last trigger activated, and this variable is now transmitted in the trigger activation trap *triggerTrap*.

PCR: 01214 Module: SWI Network affecting: No

In a Rapier G6, fitted with a fibre uplink module with all ports active, switching traffic between port 1 and the uplink caused the traffic flow to cease after a period of time depending on the volume of traffic. This issue has been resolved.

PCR: 01216 Module: STP Network affecting: No

The Rapier did not include the message age of the received BDPU message in the message age of the BDPU it transmitted. Also, the message age of the message transmitted BDPU could be less than that of the received BDPU, which contravenes IEEE 802.3d. This issue has been resolved.

PCR: 01219 Module: VLAN,SWI Network affecting: No

Reception of incorrectly tagged packets was causing corruption of the ARL table, eventually causing the switch to lock up. This issue has been resolved. Tagged packets with invalid VLAN identifiers are now discarded. The INFILTERING parameter of the SET SWITCH PORT command now defaults to ON.

PCR: 01221 Module: SWI Network affecting: No

Flow control performance has been improved.

PCR: 01225 Module: IPSEC Network affecting: No

The IPsec SA ID now wraps correctly at the 16 bit (ID = 65535) boundary. The ID is also checked to verify that it is free before it is used.

PCR: 01227 Module: PPP Network affecting: No

If PPPoE AC services were not deleted in the same order they were added, the DELETE command would return an "operation successful" message but the service would still appear in the output of the SHOW PPP PPPOE command. This issue has been resolved.

PCR: 01229 Module: SWI Network affecting: No

The CREATE CONFIG command did not include all required L3FILTER parameters in the generated script file.

PCR: 01232 Module: SWI Network affecting: No

The L3 table on the Rapier G6 is now cleared when a switch port goes down to ensure the L3 and ARP tables are consistent.

PCR: 01234 Module: SWI Network affecting: No

A switch port that was transmitting STP BPDUs and also mirroring its transmit traffic to the mirror port caused a fatal error. This issue has been resolved.

Features in 86222-06

Patch file details for Patch 86222-06 are listed in Table 19.

Table 19: Patch file details for Patch 86222-06.

Base Software Release File	86s-222.rez
Patch Release Date	30-Aug-2001
Compressed Patch File Name	86222-06.paz
Compressed Patch File Size	226776 bytes

Patch 86222-06 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01188 Module: SWI Network affecting: No

The power supply voltages of the base board PHYs on a Rapier G6 are controlled by a PHY register value, which was incorrectly set. This issue has been resolved.

PCR: 01190 Module: PIM Network affecting: No

In PIM Dense Mode, if a data stream started before PIM hello messages were exchanged, the receiver did not get the data stream. This issue has been resolved.

PCR: 01192 Module: SWI Network affecting: No

The Rapier G6 base ports sometimes experienced spurious link up or link down events. This issue has been resolved.

Features in 86222-05

Patch file details for Patch 86222-05 are listed in Table 20.

Table 20: Patch file details for Patch 86222-05.

Base Software Release File	86s-222.rez
Patch Release Date	24-Aug-2001
Compressed Patch File Name	86222-05.paz
Compressed Patch File Size	223728 bytes

Patch 86222-05 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01148 Module: SWI Network affecting: No

A39 copper uplink modules in the Rapier G6 sometimes experienced spurious link up or link down events. This issue has been resolved.

PCR: 01157 Module: CORE Network affecting: No

The enterprise MIB now supports objects for power supply monitoring.

PCR: 01162 Module: PKI Network affecting: No

Certificates containing *GeneralisedTime* with the year in YYYY format are now parsed correctly. The *keyUsage* field of certificates is now parsed correctly when only one byte has been specified. The *CRL update time* is now displayed correctly in hours. If the *username* and *password* parameters are present the *location* parameter must be present and appear before the *username* and *password* parameters. Certificates with signatures of 257 bytes are now correctly parsed. Certificates added from a configuration script are now processed correctly.

PCR: 01170 Module: IPv6 Network affecting: No

A fatal error occurred if an IPv6 interface was deleted while packets were being transmitted. The number of current interfaces was not being updated correctly when a new IPv6 interface was added. As a result, after multiple additions and deletions, no more IPv6 interfaces could be added. These issues have been resolved.

PCR: 01176 Module: PKI Network affecting: No

The CREATE CONFIG command now adds PKI certificates to the script in the same order that they were originally added to the certificate database.

PCR: 01177 Module: PKI Network affecting: No

PKI certificates are now periodically checked (once per hour) to verify that they are still valid.

PCR: 01178 Module: IPSEC Network affecting: No

IPCOMP SA's which have the reserved CPI "3" are no longer deleted by ISAKMP delete messages.

PCR: 01179 Module: SWI Network affecting: No

When a VLAN was created and then destroyed on the G6 or G6F, the VTABLE was corrupted. This has been fixed.

PCR: 01181 Module: DHCP Network affecting: No

DHCP failed to send request messages when it was in a rebinding or renewing state. This issue has been resolved.

PCR: 01185 Module: SWI Network affecting: No

In some extreme traffic conditions the switch could lock up, preventing switching of any traffic. This issue has been resolved.

PCR: 01186 Module: FIREWALL Network affecting: No

When large numbers of sessions were being handled the firewall would become overly aggressive in restricting new sessions. The *Active TCP Opens* field in the output of the SHOW FIREWALL POLICY would show a very high number (42×10^8). This issue has been resolved.

PCR: 01187 Module: IPG Network affecting: No

If the IGMP table was empty and a timeout was set, a fatal error occurred. This issue has been resolved.

Features in 86222-04

Patch file details for Patch 86222-04 are listed in Table 21.

Table 21: Patch file details for Patch 86222-04.

Base Software Release File	86s-222.rez
Patch Release Date	24-Aug-2001
Compressed Patch File Name	86222-04.paz
Compressed Patch File Size	220220 bytes

Patch 86222-04 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01124 Module: PKI Network affecting: No

Message protection validation failures would occur intermittently. This issue has been resolved.

PCR: 01136 Module: ISAKMP Network affecting: No

ISAKMP now interoperates with other vendor's products in aggressive mode exchanges.

PCR 01138 Module: CORE, SWI Network affecting: No

Support has been added for the 8624XL-80 switch with -48VDC power supply.

PCR: 01152 Module: FIREWALL Network affecting: No

In a dual policy configuration, the firewall would lock up under load. The firewall would also mistakenly report SYN attacks. These issues have been resolved.

PCR: 01159 Module: PIM Network affecting: No

The CREATE CONFIG command generated duplicate PIM interface configuration command lines. This issue has been resolved.

PCR: 01162 Module: PKI Network affecting: No

Certificates containing *GeneralisedTime* with the year in YYYY format are now parsed correctly. The *keyUsage* field of certificates is now parsed correctly when only one byte has been specified. The *CRL update time* is now displayed correctly in hours. If the *username* and *password* parameters are present the *location* parameter must be present and appear before the *username* and *password* parameters.

PCR: 01165 Module: DHCP Network affecting: No

The DHCP server now correctly allocates addresses to clients running Apple Open Transport 2.5.1 or 2.5.2.

PCR: 01166 Module: FIREWALL Network affecting: No

Both public and private access could be configured on the same interface on a policy. This issue has been resolved.

PCR: 01167 Module: ENCO Network affecting: No

RSA encryption is now periodically suspended to ensure other processes get some CPU time during large RSA calculations.

PCR: 01169 Module: ISAKMP Network affecting: No

The CREATE ISAKMP command now checks that the key specified by the LOCALRSAKEY parameter actually exists in the ENCO module.

PCR: 01171 Module: ETH, TRIGGER Network affecting: No

The INTERFACE parameter of the CREATE TRIGGER and SET TRIGGER commands now supports Ethernet interfaces. Ethernet interface events can now generate triggers.

PCR: 01173 Module: Telnet Network affecting: No

The Telnet server's listen port can now be configured to a number in the range 1 to 65535, excluding any ports already assigned as listen ports.

PCR: 01174 Module: Firewall Network affecting: No

The CREATE CONFIG command sometimes generated scripts for rule commands with GBLIP=0.0.0.0 when this was not necessary. This issue has been resolved.

Features in 86222-01

Patch file details for Patch 86222-01 are listed in Table 22.

Table 22: Patch file details for Patch 86222-01.

Base Software Release File	86s-222.rez
Patch Release Date	11-Jul-2001
Compressed Patch File Name	86222-01.paz
Compressed Patch File Size	187124 bytes

Patch 86222-01 includes the following enhancement for Software Release 2.2.2:

PCR: 01100 Module: DHCP Network affecting: No

The DHCP server identified the wrong port numbers for incoming DHCP requests causing DHCP replies to be sent to the wrong port. This issued has been resolved.

PCR: 01102 Module: IPG Network affecting: No

The IP flow cache occasionally generated a watchdog fatal error. This issued has been resolved.

PCR: 01102 Module: SWI Network affecting: No

Deleting entries from an L3 table occasionally resulted in a watchdog fatal error. This issue has been resolved.

PCR: 01106 Module: PKI Network affecting: No

PKI enrolment no longer causes message validation to fail.

PCR: 01119 Module: IPV6 Network affecting: No

Repeated addition and deletion of an address with the VALID parameter set to or from an IPV6 interface caused a fatal error. This issue has been corrected. The VALID parameter specifies the life of the address, and defaults to INFINITE. The address is deleted when the lifetime expires. The PREF parameter specifies the time that the address is the preferred address of the interface, and defaults to INFINITE. PREF must be less than or equal to VALID. IPV6 now checks and ensures that if either PREF or VALID is specified, PREF is less than or equal to VALID. When an address is deleted the timers are now correctly cleared.

PCR: 01120 Module: IPG Network affecting: No

IP sometimes passed the wrong port number to PIM, causing PIM to process the wrong port number in its routing table. This issued has been resolved.

Availability

Patches can be downloaded from the Software Updates area of the Allied Telesyn web site at *www.alliedtelesyn.co.nz/support/updates/patches.html*. A licence or password is not required to use a patch.